WLM-3500

Wireless ADSL2+ router

User Manual

Version: 1.0

TABLE OF CONTENTS

1 KEY FEATURES 4
2 PACKAGE CONTENTS 5
3 PRODUCT LAYOUT 6
4 SYSTEM REQUIREMENTS 8
5 WLM-3500 PLACEMENT 9
6 SETUP LAN, WAN 9
7 PC NETWORK ADAPTER SETUP 10
8 BRINGING UP THE WLM-3500 13
9 INITIAL SETUP WLM-3500 13
10 CONFIGURATION WIZARD 23
11 WIRELESS SETTINGS 25
12 FIREWALL SETTINGS 35
13 ADVANCED SETTINGS 42
14 TOOLBOX SETTINGS 54

Introduction

Congratulations on your purchase of the WLM-3500 Wireless ADSL2+ Modem. The WLM-3500 is fully compliant with 802.11n, 802.11g & 802.11b. This modem provides the best performance when used in combination with 802.11n client adapters.

The WLM-3500 is not only a Modem or Wireless Access Point, but can also be used to connect wired-Ethernet devices.

For data protection and privacy, the WLM-3500 can encode all wireless transmissions with WEP, WPA, and WPA2 encryption. By default, the modem is secured with a WPA2 (AES) encryption key. (The WPA2-key is printed on the label underneath the modem.)

With a built-in DHCP Server & powerful SPI firewall the WLM-3500 protects your computers against intruders and known Internet attacks, and also provides safe VPN pass-through.

1 Key Features

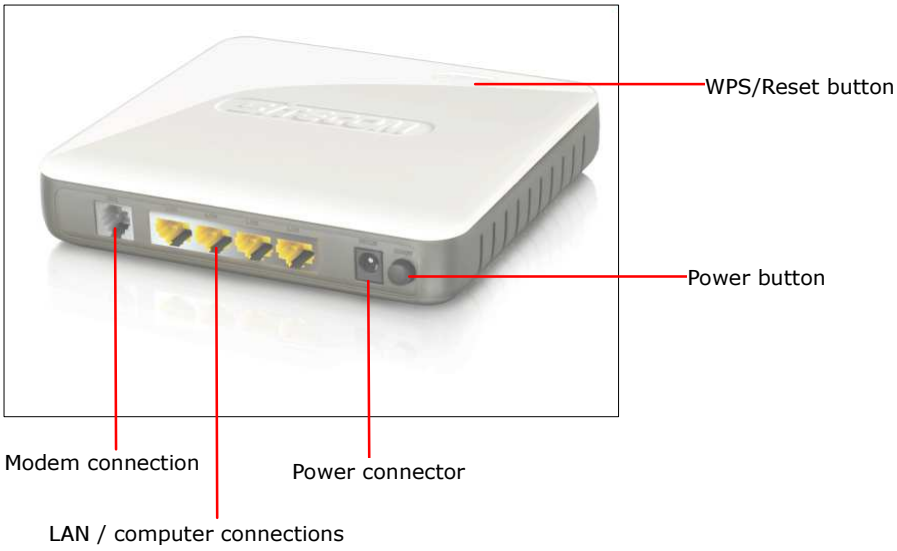
Features	Advantages
IEEE 802.11g compliant	**Fully Interoperable with IEEE 802.11b / IEEE802.11g compliant devices**
Based on 802.11n technology	**Up to 6 times faster than regular 802.11g.** **(in combination with a 802.11n wireless adapter)**
Four 10/100 Mbps Fast Ethernet Port (Auto-Crossover)	**To connect four wired PC's as well.**
Firewall supports Virtual Server Mapping, DMZ, IP Filter, ICMP Blocking, SPI	**Avoids the attacks of Hackers or Viruses from Internet**
Support 802.1x authenticator, 802.11i (WPA/WPA2, AES), VPN pass-through	**Provide mutual authentication (Client and dynamic encryption keys to enhance security**
Integrated modem (Annex A)	**Fully compatible with the fastest ADSL2+ connections up-to-date.**

2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped back in its original package.

1. WLM-3500 modem/router
2. 220V ~ 240V Power Adapter
3. Quick Install Guide
4. CD (User's Manual)
5. Warranty card
6. UTP cable

3 Product Layout



Port	Description
ADSL	Connect your telephone/ADSL cable this port
LAN	Connect the cable from your PC or network device to this ports.
Power connector	Connect your power adapter to this port.
Power button	Turn the modem On or Off.

Back label

The back label describes the corresponding LED indications and port functionality.

LED	Description
Power	Lights up when powered ON. Blinks on TEST/RESET
ADSL	Lights up when an ADSL cable is connected.
Internet	Lights up when internet connection is UP.
WLAN	Lights up in Blue when WLAN is enabled. Blinks on traffic
OPS	Blinks when OPS mode is on
LAN1~4	When a LAN cable is connected the corresponding light lights up.

4 System Requirements

To begin using the WLM-3500, make sure you meet the following as minimum requirements:

- PC/Notebook.
- 1 Free Ethernet port.
- Wi-Fi card/USB dongle (802.11 b/g/n) – optional.
- Annex A, ADSL internet connection.
- PC with a Web-Browser (Internet Explorer, Safari, Firefox, Opera)
- Ethernet compatible CAT5 cables.

5 WLM-3500 Placement

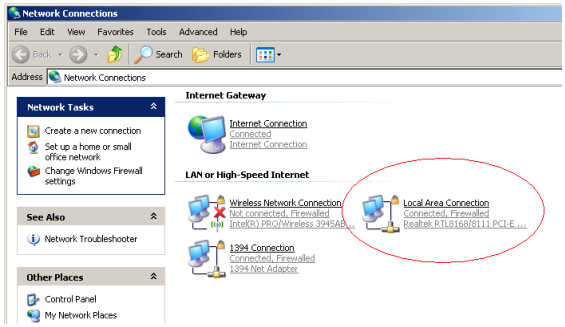
You can place the WLM-3500 on a desk or other flat surface, or you can mount it on a wall. For optimal performance, place your Wireless Broadband Modem/Router in the center of your office (or your home) in a location that is away from any potential source of interference, such as a metal wall or microwave oven. This location must be close to a power connection and the ADSL/phone line should not be over 2 meters long.

6 Setup LAN, WAN

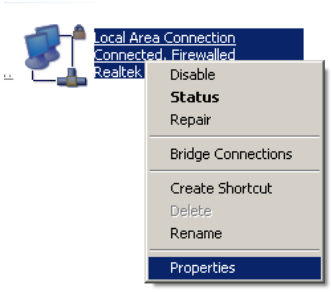
7 PC Network Adapter setup

Windows XP

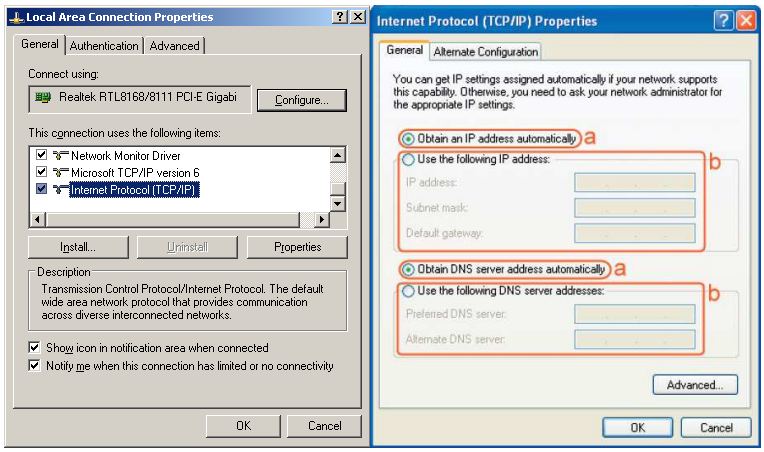
- Go to [*Start Menu*], → [*Control panel*], → [*Network Connections*].



- Right-mouse-click on the [*Local Area Connection]*) icon, and select [*properties*]



- Select [*Internet Protocol (TCP/IP)*] =>Click [*Properties*].

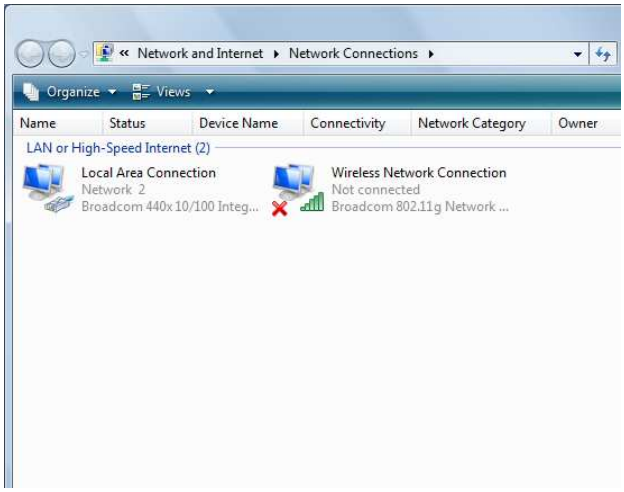

Local Area Connection Properties
General Authentication Advanced
Connect using:
Realtek RTL8168/8111 PCI-E Gigabi
Configure...
This connection uses the following items:
Network Monitor Driver
Microsoft TCP/IP version 6
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
Notify me when this connection has limited or no connectivity
OK Cancel
Internet Protocol (TCP/IP) Properties
General Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK Cancel

- Select the [*General*] tab.

  The WLM-3500 supports DHCP. Please select both [*Obtain an IP address automatically*] and [*Obtain DNS server address automatically*].

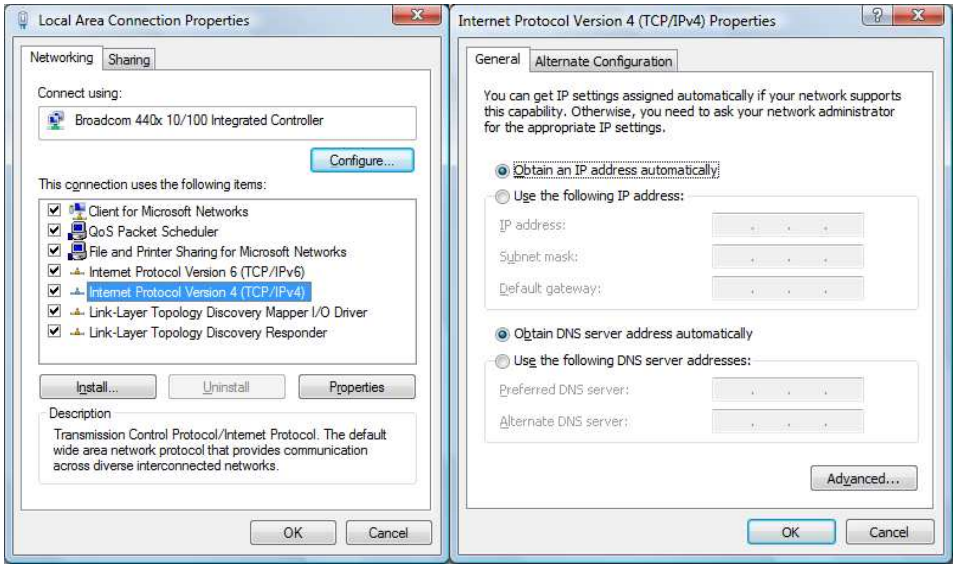
Windows Vista/Windows 7

- Go to [*Start Menu*], → [*Control panel*], → [*View network status and tasks*], -> [*Manage network connections*].



- Right-mouse-click on the [*Local Area Connection*]) icon, and select [*properties*]

- Select [*Internet Protocol Version 4 (TCP/IPv4)*], and Click [*Properties*].


Local Area Connection Properties
Networking
Sharing
Connect using:
Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

- Open the [*General*] tab.

  The WLM-3500 supports DHCP. Please select both [*Obtain an IP address automatically*] and [*Obtain DNS server address automatically*].

8 Bringing up the WLM-3500

Connect the supplied power-adapter to the power inlet port and connect it to a wall outlet. Press the Power-Button to turn the modem on.

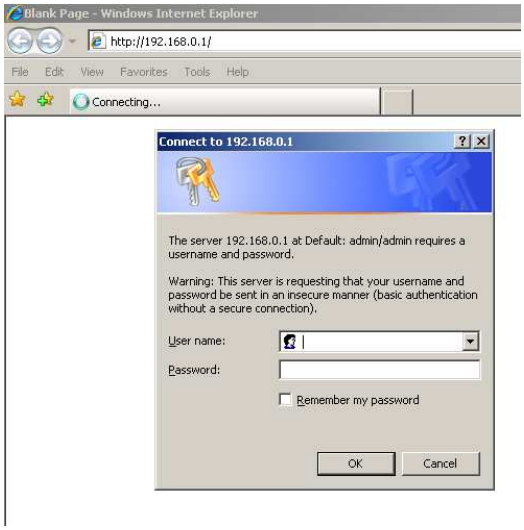
The WLM-3500 automatically enters the self-test phase. During self-test phase, the Power LED will blink briefly, and then will be lit continuously to indicate that this product is in normal operation.

9 Initial Setup of the WLM-3500

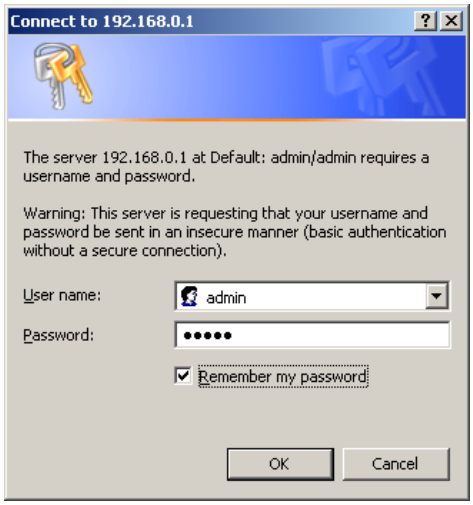
LOGIN procedure

1. OPEN your browser (e.g. Internet Explorer).

2. Type http://192.168.0.1 in address bar and press [Enter]


Blank Page - Windows Internet Explorer
http://192.168.0.1/
File Edit View Favorites Tools Help
Connecting...
Connect to 192.168.0.1
The server 192.168.0.1 at Default: admin/admin requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

4. Type user name and password. The default username is “admin”. The default password can be found on the backlabel of the device.

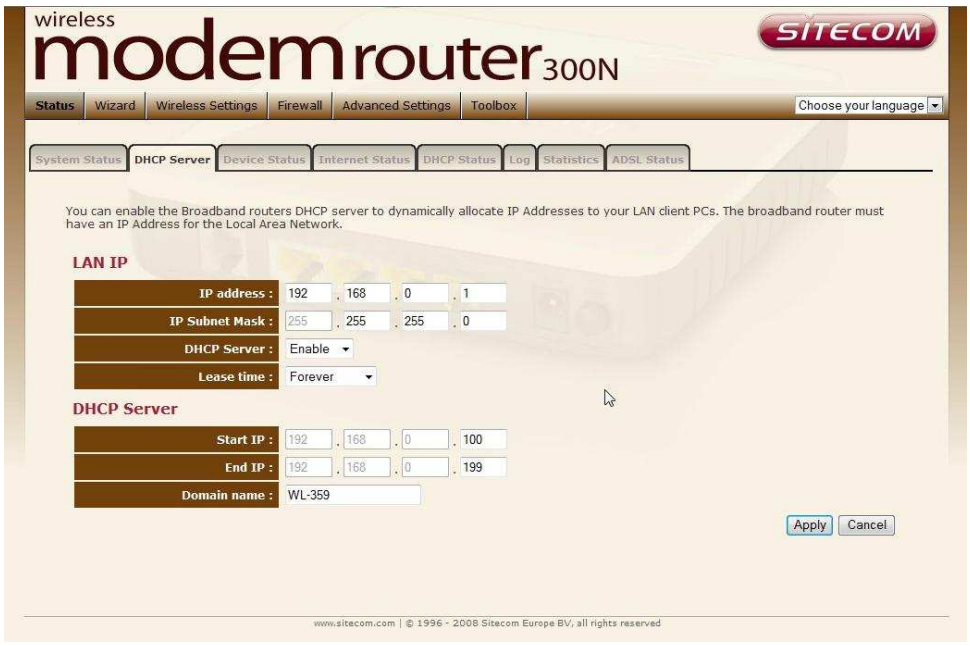

Connect to 192.168.0.1
The server 192.168.0.1 at Default: admin/admin requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

3. Click **OK**.
4. You will see the home page of the WLM-3500.

The System status section allows you to monitor the current status of your router: the UP time, hardware information, serial number as well as firmware version information is displayed here.

LAN settings

The LAN tab gives you the opportunity to change the IP settings of the WLM-3500.


wireless
modem router 300N
SITECOM
Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
System Status
DHCP Server
Device Status
Internet Status
DHCP Status
Log
Statistics
ADSL Status
You can enable the Broadband routers DHCP server to dynamically allocate IP Addresses to your LAN client PCs. The broadband router must have an IP Address for the Local Area Network.
LAN IP
IP address : 192 . 168 . 0 . 1
IP Subnet Mask : 255 . 255 . 255 . 0
DHCP Server : Enable
Lease time : Forever
DHCP Server
Start IP : 192 . 168 . 0 . 100
End IP : 192 . 168 . 0 . 199
Domain name : WL-359
Apply
Cancel
www.sitecom.com | © 1996 - 2008 Sitecom Europe BV, all rights reserved

Click **<Apply>** at the bottom of this screen to save any changes.

IP address 192.168.0.1. It is the router's LAN IP address (Your LAN clients default gateway IP address).

IP Subnet Mask 255.255.255.0 Specify a Subnet Mask for your LAN segment.

DHCP Server Enabled by default. You can enable or disable the DHCP server. When DHCP is disabled no ip-addresses are assigned to clients and you have to use static ip-addresses. When DHCP server is enabled your computers will be assigned an ip-address automatically until the lease time expires.

Lease Time Forever. In the Lease Time setting you can specify the time period that the DHCP lends an IP address to your LAN clients. The DHCP will change your LAN client's IP address when this time threshold period is reached.

IP Address Pool You can select a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients.

***Note**: default IP range 192.168.0.100 ←→ 192.168.0.199. If you want your PC(s) to have a static/fixed IP address, then you'll have to choose an IP address outside this IP address Pool*

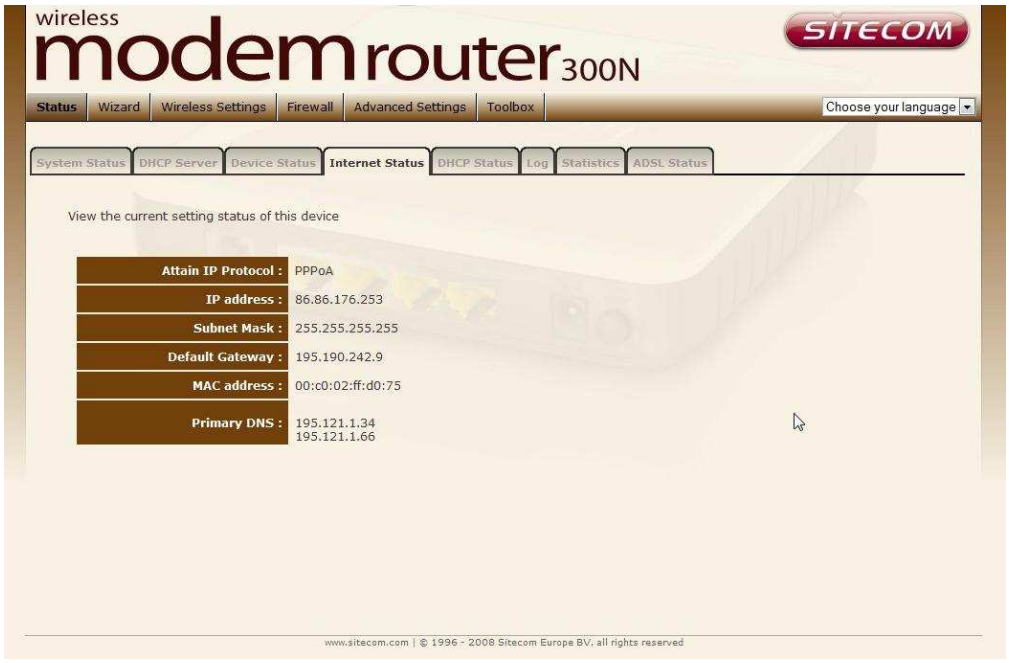
Domain Name You can specify a Domain Name for your LAN. Or just keep the default (WLM-xxxx).

Device Status

View the Broadband modem/router's current configuration settings. Device Status displays the configuration settings you've configured in the Wizard / Basic Settings / Wireless Settings section.

Internet Status

This page displays whether the ADSL port is connected to an ADSL service provider. It also displays the router's WAN IP address, Subnet Mask, and ISP Gateway as well as MAC address, the Primary DNS. Press **Renew** button to renew your WAN IP address.



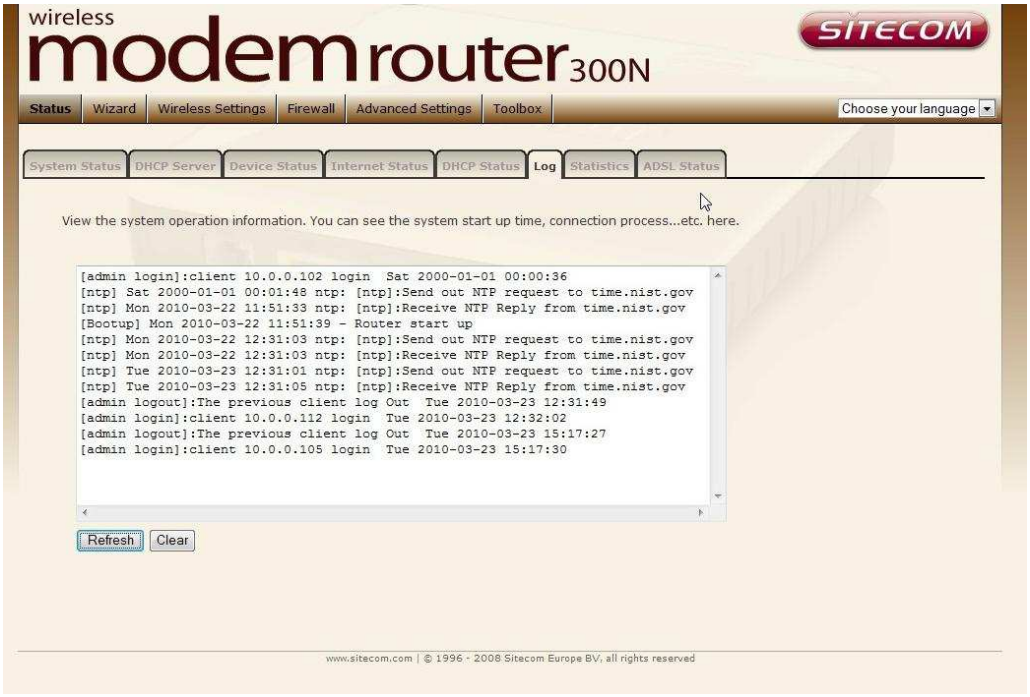
DHCP Client Status

This page shows all DHCP clients (LAN PCs) currently connected to your network. The table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

Use the **Refresh** button to update the available information.

WLM-3500 Log

View the operation log of the **WLM-3500**. This page shows the current system log of the Broadband modem/router. It displays any event occurred after system start up. At the bottom of the page, the system log can be saved **<Save>** to a local file for further processing or the system log can be cleared **<Clear>** or it can be refreshed **<Refresh>** to get the most updated information. When the system is powered down, the system log will disappear if not saved to a local file.

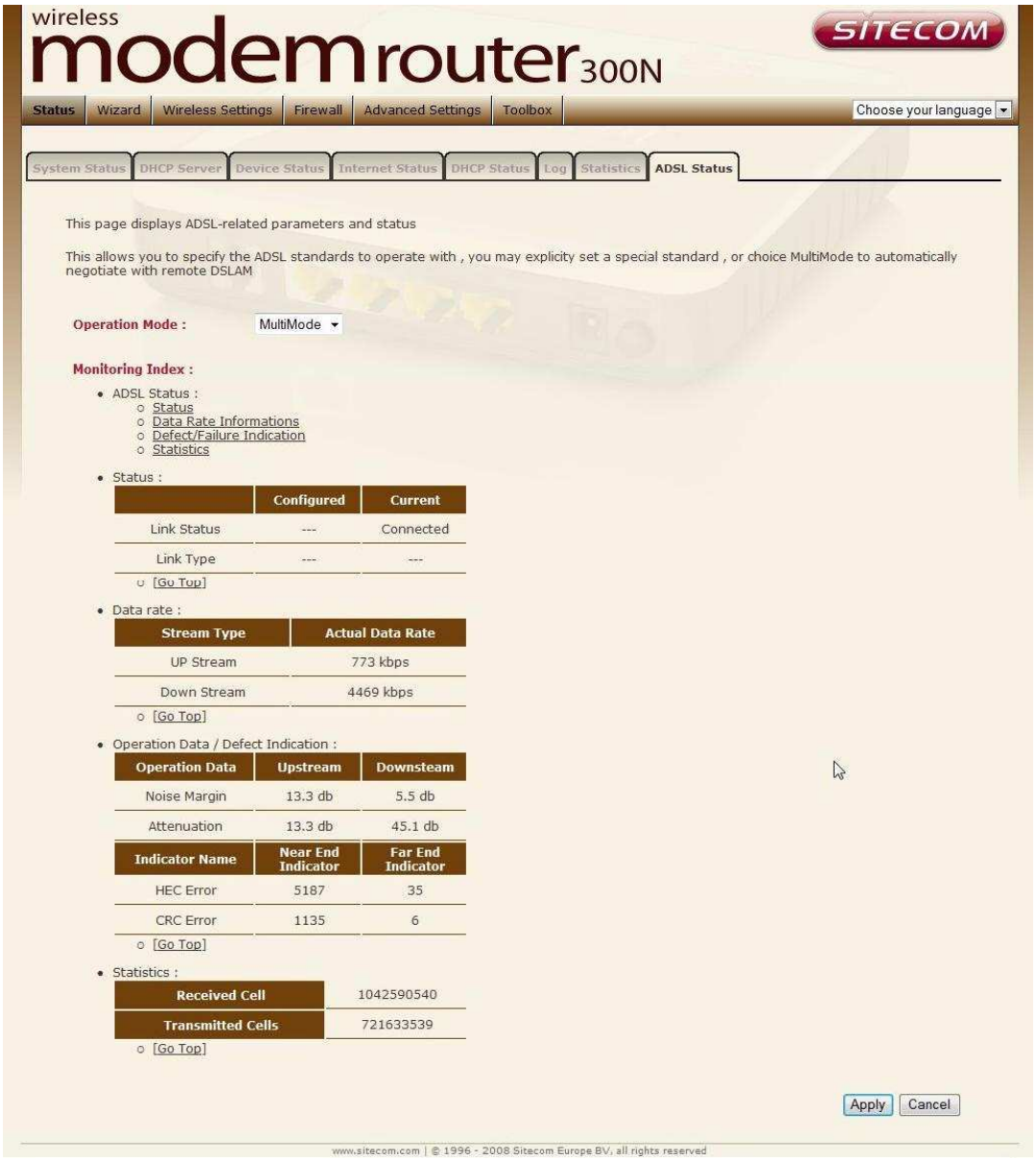

wireless
modem router 300N
SITECOM
Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
System Status
DHCP Server
Device Status
Internet Status
DHCP Status
Log
Statistics
ADSL Status
View the system operation information. You can see the system start up time, connection process...etc. here.
[admin login]:client 10.0.0.102 login Sat 2000-01-01 00:00:36
[ntp] Sat 2000-01-01 00:01:48 ntp: [ntp]:Send out NTP request to time.nist.gov
[ntp] Mon 2010-03-22 11:51:33 ntp: [ntp]:Receive NTP Reply from time.nist.gov
[Bootup] Mon 2010-03-22 11:51:39 - Router start up
[ntp] Mon 2010-03-22 12:31:03 ntp: [ntp]:Send out NTP request to time.nist.gov
[ntp] Mon 2010-03-22 12:31:03 ntp: [ntp]:Receive NTP Reply from time.nist.gov
[ntp] Tue 2010-03-23 12:31:01 ntp: [ntp]:Send out NTP request to time.nist.gov
[ntp] Tue 2010-03-23 12:31:05 ntp: [ntp]:Receive NTP Reply from time.nist.gov
[admin logout]:The previous client log Out Tue 2010-03-23 12:31:49
[admin login]:client 10.0.0.112 login Tue 2010-03-23 12:32:02
[admin logout]:The previous client log Out Tue 2010-03-23 15:17:27
[admin login]:client 10.0.0.105 login Tue 2010-03-23 15:17:30
Refresh
Clear
www.sitecom.com | © 1996 - 2008 Sitecom Europe BV, all rights reserved

Statistics

This page shows the statistics for the wireless, LAN, and WAN interfaces.

ADSL Status

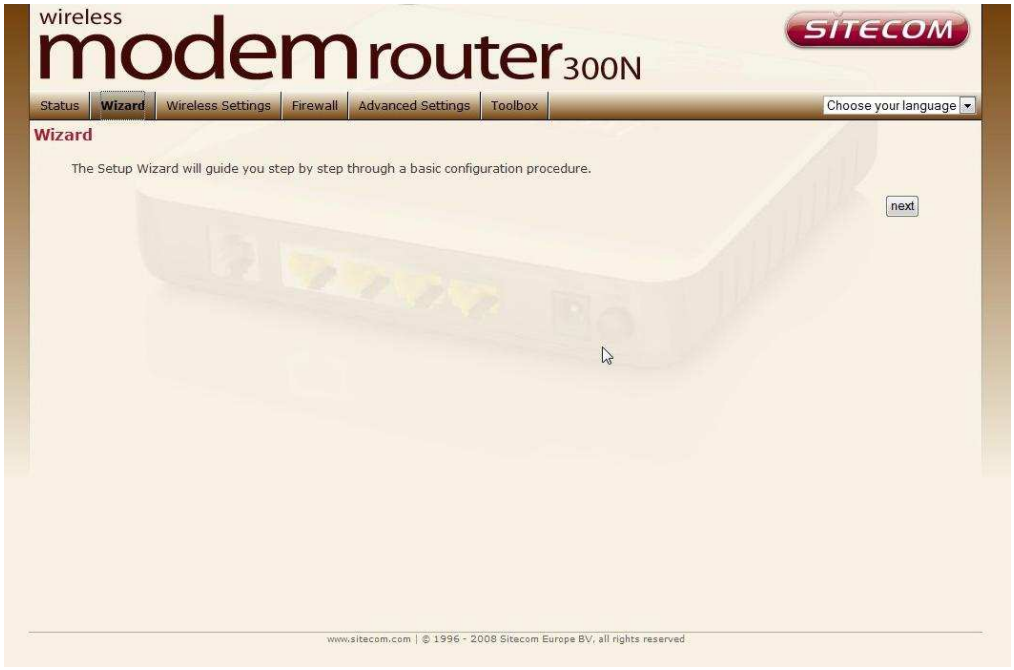
This page shows the current operation mode, status of your ADSL connection, the data rate and the quality of your ADSL link.



Operation mode allows manual selection of the ADSL mode.

10 Configuration Wizard

Click **Wizard** to configure the modem. The Setup wizard will now be displayed; check that the adsl line is connected and click **Next.**



Select your country from the Country list. Select your internet provider. Click **Next.**

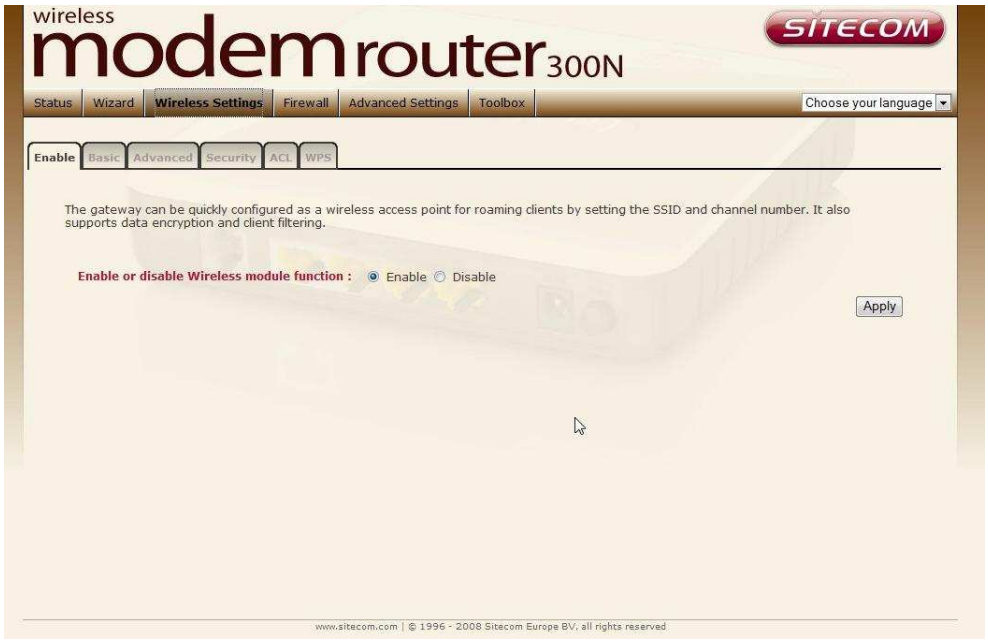
Depending on the chosen provider, you may need to enter your user name and password or hostname in the following window. After you have entered the correct information, click **Next**.

Click **APPLY** to complete the configuration.

11 Wireless Settings

You can set parameters that are used for the wireless stations to connect to this router. The parameters include Mode, ESSID, Channel Number and Associated Client.

Wireless Function



Enable or Disable Wireless function here. Click **Apply** and wait for module to be ready & loaded.

Basic Settings

802.11 Mode Allows you to set the AP fixed at 802.11b or 802.11g mode. You can also select B+G+N mode to allow 802.11b, 802.11g and 802.11n clients at the same time.

Band 20/40 MHz Allows automatic detection of the operation bandwidth between 20 and 40 MHz.

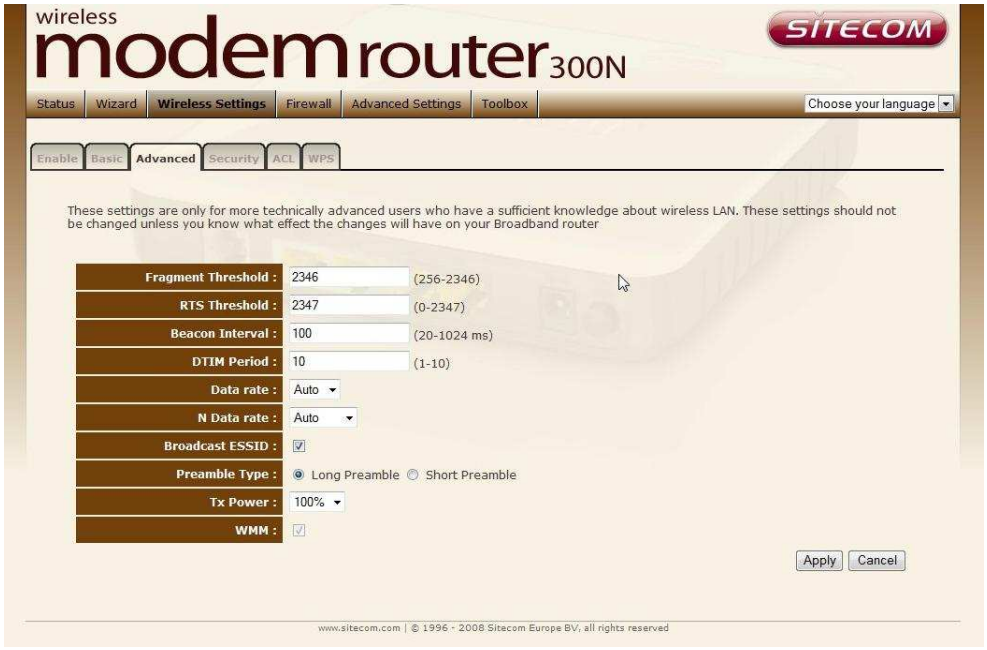
ESSID This is the name of the wireless signal which is broadcasted. All the devices in the same wireless LAN should have the same ESSID.

Channel Number The channel used by the wireless LAN. All devices in the same wireless LAN should use the same channel.

Extension channel This is the optional channel for use. Setting the Bandwidth to 20/40 MHz allows you to use this extension channel as the secondary channel for doubling the bandwidth of your wireless network.

Advanced Settings

This tab allows you to set the advanced wireless options. The options included are Authentication Type, Fragment Threshold, RTS Threshold, Beacon Interval, and Preamble Type. You should not change these parameters unless you know what effect the changes will have on the router.



Fragment Threshold "Fragment Threshold" specifies the maximum size of a packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.

RTS Threshold When the packet size is smaller then the RTS threshold, the wireless router will not use the RTS/CTS mechanism to send this packet.

Beacon Interval is the interval of time that this wireless router broadcasts a beacon. A Beacon is used to synchronize the wireless network.

DTIM period is a countdown mechanism for WLAN Access Points changing this value will affect your wireless performance and may improve stability.

Preamble Type The "Long Preamble" can provide better wireless LAN compatibility while the "Short Preamble" can provide better wireless LAN performance.

Broadcast ESSID If you enabled "Broadcast ESSID", every wireless station located within the coverage of this access point can discover this access point

easily. If you are building a public wireless network, enabling this feature is recommended. Disabling "Broadcast ESSID" can provide better security.

Tx Power Use this option to adjust the transmit power of the wireless interface.

WMM Wi-Fi Multi Media if enabled supports QoS for experiencing better audio, video and voice in applications.

Security

This Access Point provides complete wireless LAN security functions, included are WEP, WPA with pre-shared key and WPA2 with pre-shared key. With these security functions, you can prevent illegal access to your wireless LAN. Please make sure your wireless stations use the same security function, and are setup with the same security key.

Disable

When you choose to disable encryption, it is very insecure to operate the WLM-3500.

WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself and enter it. You can enter four WEP keys and select one of them as a default key. Then the router can receive any packets encrypted by one of the four keys.

Key Length You can select the WEP key length for encryption, 64-bit or 128-bit. The larger the key will be the higher level of security is used, but the throughput will be lower.

Key Format You may select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the "A-F", "a-f" and "0-9" range) to be the WEP Key.

Key1 - Key4 The WEP keys are used to encrypt data transmitted in the wireless network. Use the following rules to setup a WEP key on the device. 64-bit WEP: input 10-digits Hex values (in the "A-F", "a-f" and "0-9" range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the "A-F", "a-f" and "0-9" range) or 13-digit ASCII characters as the encryption keys.

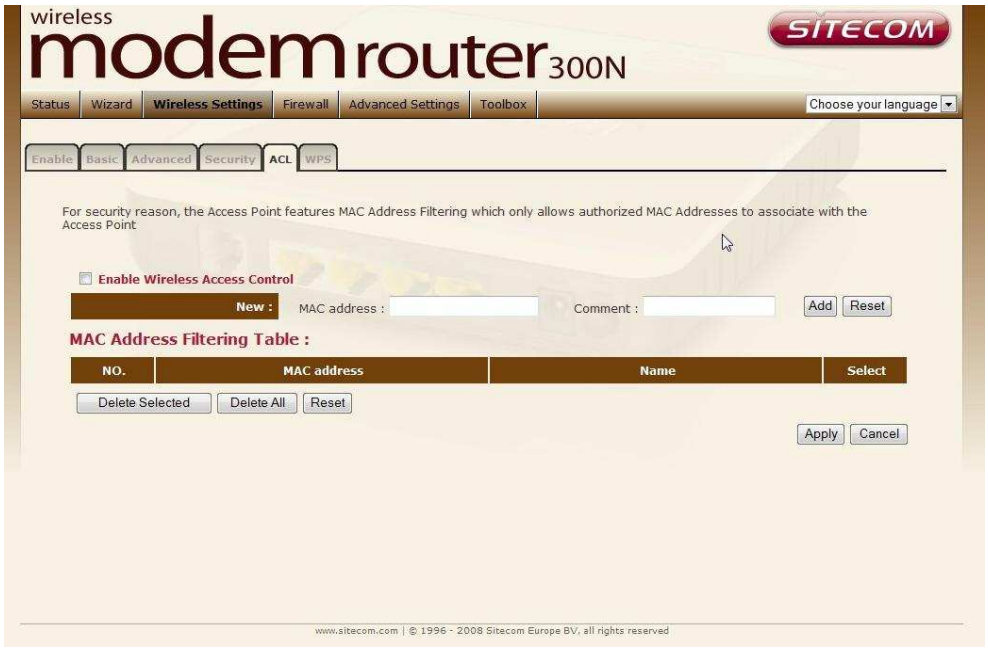
Click <Apply> at the bottom of the screen to save the above configurations. You can now configure other sections by choosing Continue, or choose Apply to apply the settings and reboot the device.

WPA Pre-shared Key

Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be cracked by hackers. This is the best security available.

ACL

This wireless router supports MAC Address Control, which prevents unauthorized clients from accessing your wireless network.



Enable wireless access control Enables the wireless access control function

Adding an address into the list Enter the "MAC Address" of the wireless station to be added and then click "Apply". The wireless station will now be added. If you are having any difficulties filling in the fields, just clear the MAC Address.

WPS

Wi-Fi Protected Setup (WPS) is the simplest way to establish a connection between the wireless clients and the wireless router. You don't have to select the encryption mode and fill in a long encryption passphrase every time when you try to setup a wireless connection. You only need to press a button on both wireless client and wireless router, and WPS will do the rest for you.

The wireless router supports two types of WPS: WPS via Push Button and WPS via PIN code. If you want to use the Push Button, you have to push a specific button on the wireless client or in the utility of the wireless client to start the WPS mode, and switch the wireless router to WPS mode. You can simply push the WPS button of the wireless router, or click the 'Start to Process' button in the web configuration interface. If you want to use the PIN code, you have to know the PIN code of the wireless client and switch it to WPS mode, then fill-in the PIN code of the wireless client through the web configuration interface of the wireless router.

WPS Check the box to enable WPS function and uncheck it to disable the WPS function.

WPS Current Status If the wireless security (encryption) function of this wireless router is properly set, you'll see a 'Configured' message here. Otherwise, you'll see 'UnConfigured'.

Self Pin Code This is the WPS PIN code of the wireless router. You may need this information when connecting to other WPS-enabled wireless devices.

SSID This is the network broadcast name (SSID) of the router.

Authentication Mode It shows the active authentication mode for the wireless connection.

Passphrase Key It shows the passphrase key that is randomly generated by the wireless router during the WPS process. You may need this information when using a device which doesn't support WPS.

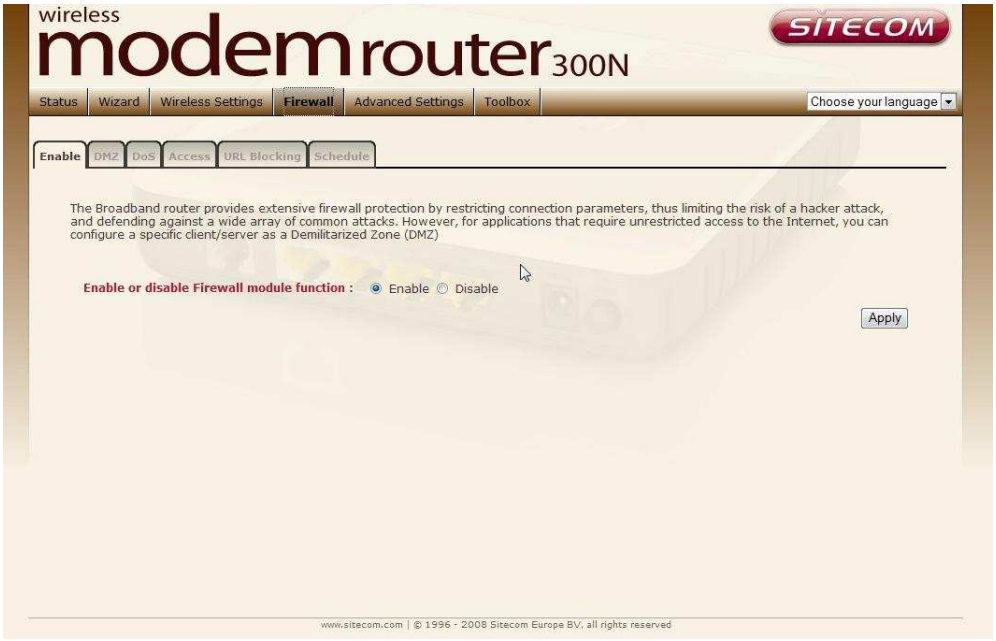
WPS via Push Button Press the button to start the WPS process. The router will wait for the WPS request from the wireless devices within 2 minutes.

WPS via PIN You can fill-in the PIN code of the wireless device and press the button to start the WPS process. The router will wait for the WPS request from the wireless device within 2 minutes.

12 Firewall Settings

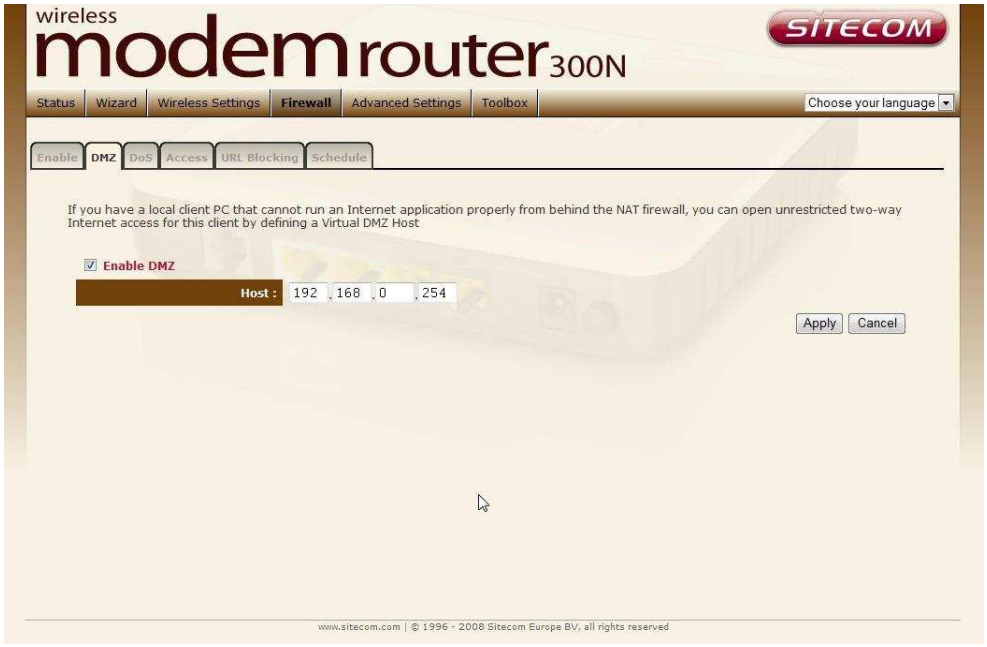
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attacks, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ).

Note: To enable the Firewall settings select Enable and click Apply.


wireless
modem router 300N
SITECOM
Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
Enable
DMZ
DoS
Access
URL Blocking
Schedule
The Broadband router provides extensive firewall protection by restricting connection parameters, thus limiting the risk of a hacker attack, and defending against a wide array of common attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server as a Demilitarized Zone (DMZ)
Enable or disable Firewall module function :
Enable
Disable
Apply
www.sitecom.com | © 1996 - 2008 Sitecom Europe BV, all rights reserved

DMZ

If you have a client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, then you can open up the firewall restrictions to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets going to your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) going to your WAN IP address to a particular LAN client/server.



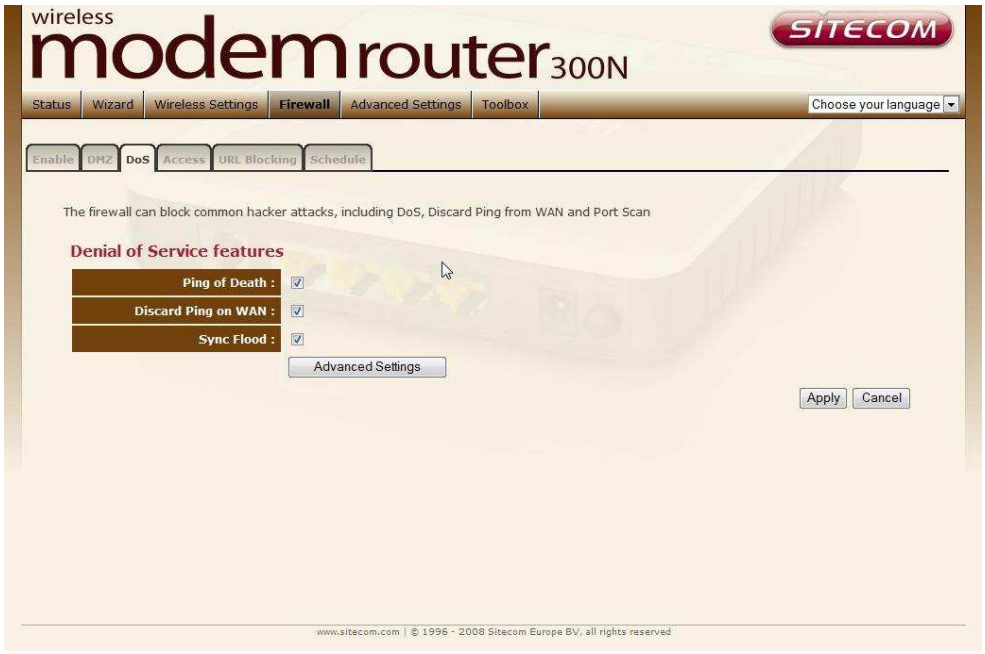
Enable DMZ Enable/disable DMZ

Host Fill in the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above.

Click **<Apply>** at the bottom of the screen to save the above configurations.

Denial of Service (DoS)

The Broadband router's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur the router can log the events.



Ping of Death blocks basic hacker attacks (DOS, Sync flood, port scan)

Discard Ping to WAN interface The router's WAN port will not respond to any Ping requests

Stateful packet inspection allows the user to manually determine which packets should be scanned.

Access

You can restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.). Access Control allows users to define the traffic type permitted in your LAN. You can control which PC client can have access to these services.

Deny If you select "Deny" then all clients will be allowed to access Internet accept for the clients in the list below.

Allow If you select "Allow" then all clients will be denied to access Internet accept for the PCs in the list below.

Filter client PCs by IP Fill in "IP Filtering Table" to filter PC clients by IP.

Add PC You can click Add PC to add an access control rule for users by IP addresses.

Remove PC If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button.

Filter client PC by MAC Check “Enable MAC Filtering” to enable MAC Filtering.

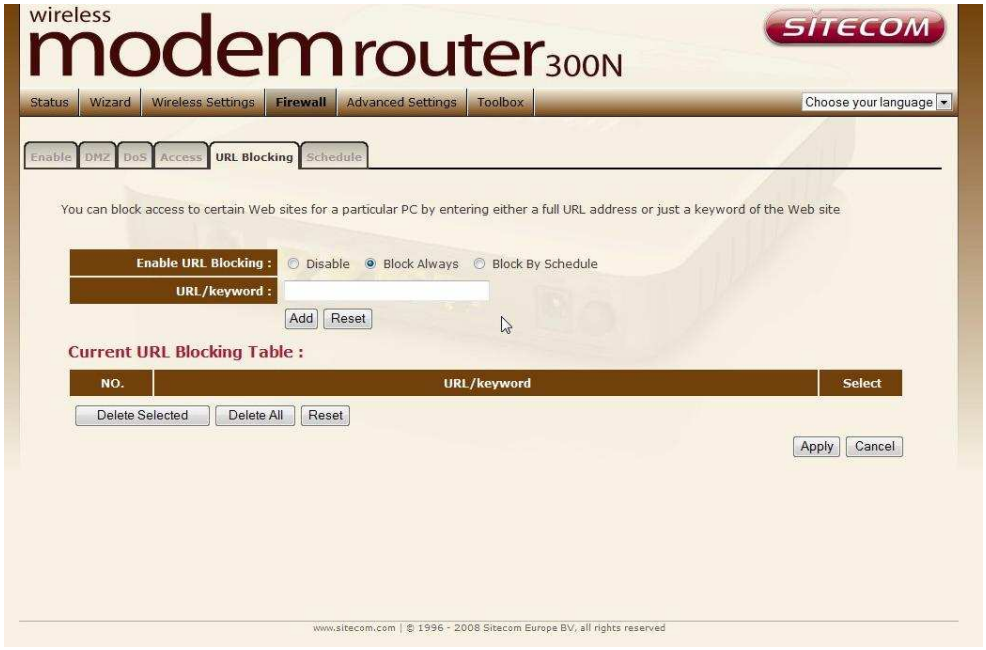
Add PC Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.

Remove PC If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want to remove all PCs from the table, just click the "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

Click <**Apply**> at the bottom of the screen to save the above configuration.

URL block

You can block access to some Web sites from particular PCs by entering a full URL address or just keywords of the Web site.



Enable URL Blocking Enable/disable URL Blocking

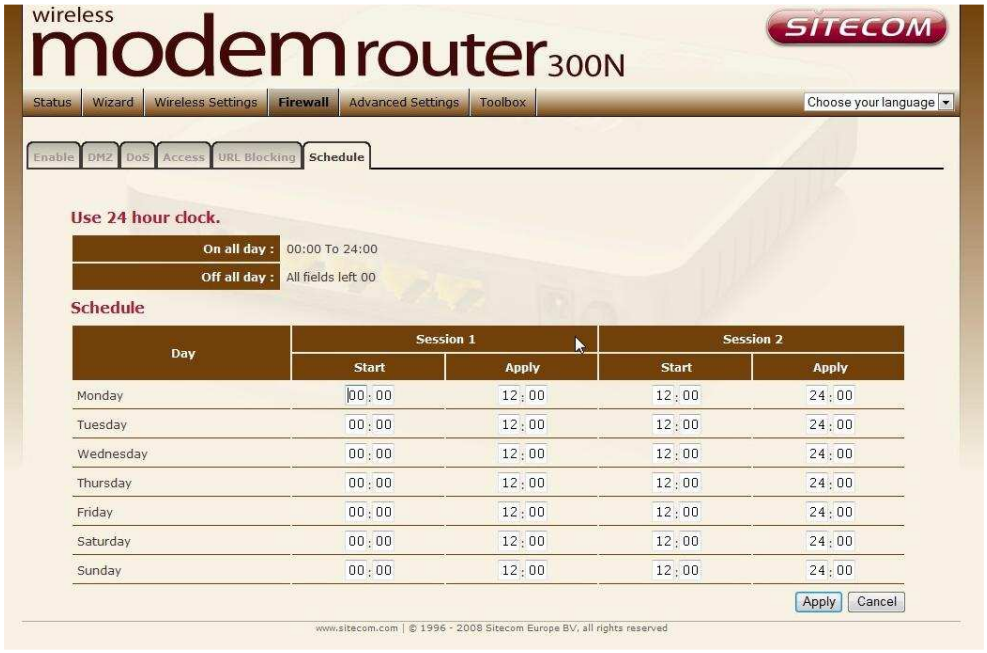
Add URL Keyword Fill in "URL/Keyword" and then click "Add". You can enter the full URL address or the keyword of the web site you want to block.

Remove URL Keyword If you want to remove some URL keywords from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keywords from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click "Reset".

Click <**Apply**> at the bottom of the screen to save the above configurations

Schedule

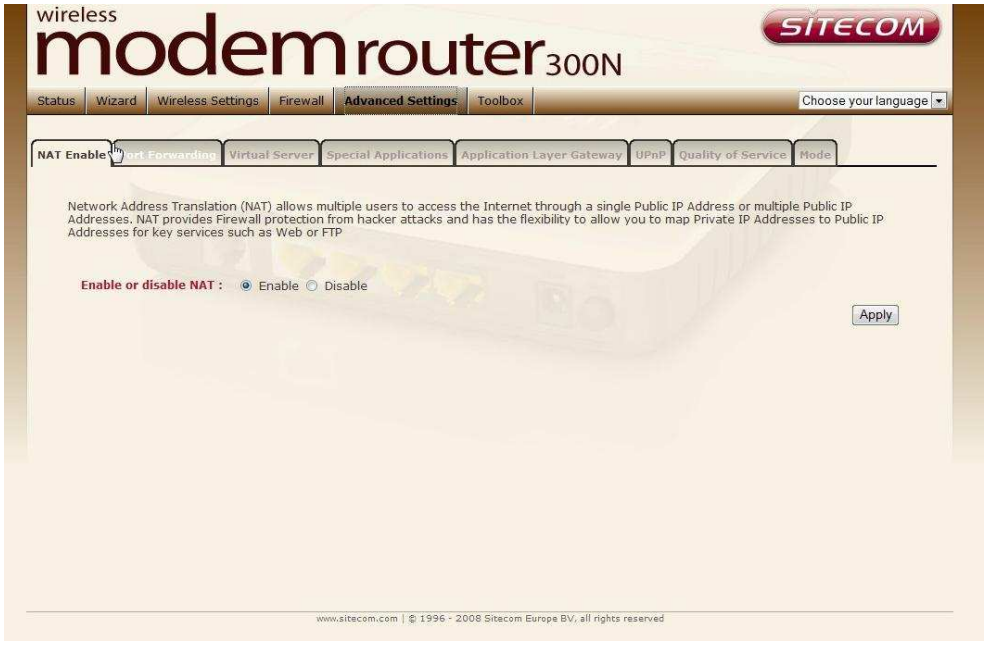
Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.



Click <**Apply**> at the bottom of the screen to save the above configurations

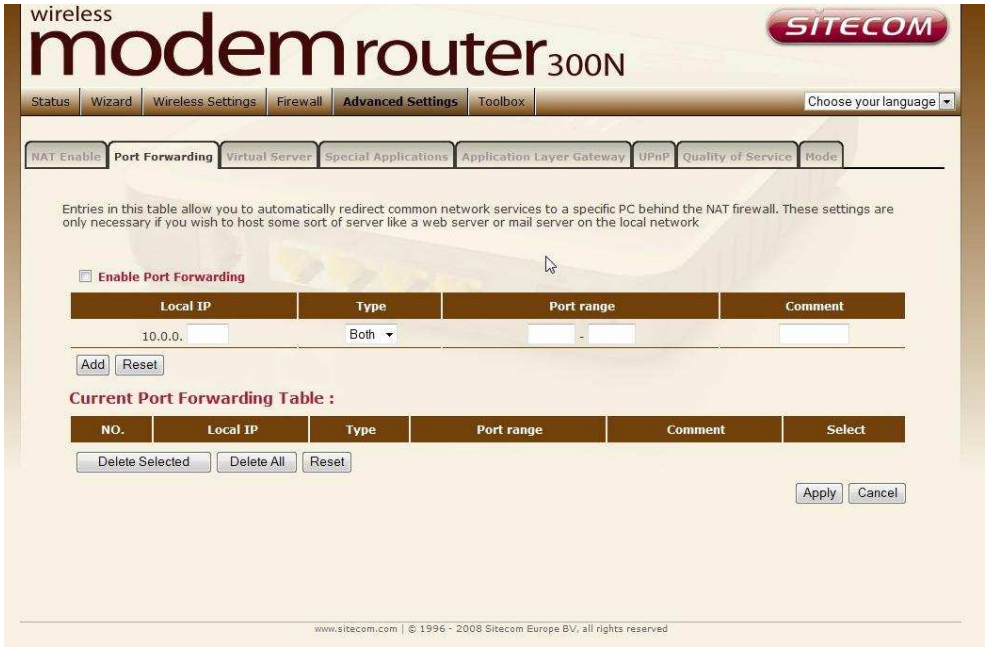
13 Advanced Settings

Network Address Translation (NAT) allows multiple users at your local site to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. Select Disable to disable the NAT function.


wireless
modem router 300N
SITECOM
Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
NAT Enable
Port Forwarding
Virtual Server
Special Applications
Application Layer Gateway
UPnP
Quality of Service
Mode
Network Address Translation (NAT) allows multiple users to access the Internet through a single Public IP Address or multiple Public IP Addresses. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Web or FTP
Enable or disable NAT :
Enable
Disable
Apply
www.sitecom.com | © 1996 - 2008 Sitecom Europe BV, all rights reserved

Port Forwarding

Multiple connections are required by some applications, such as internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.



Enable Port Forwarding Enable Port Forwarding.

Local IP This is the LAN client/host IP address that the Public Port number packet will be sent to.

Port Range This is the port range that has to be opened for your application (for the above Local IP host).

Type Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "both" setting. Public Port Enter the

service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN

Comment The description of this setting.

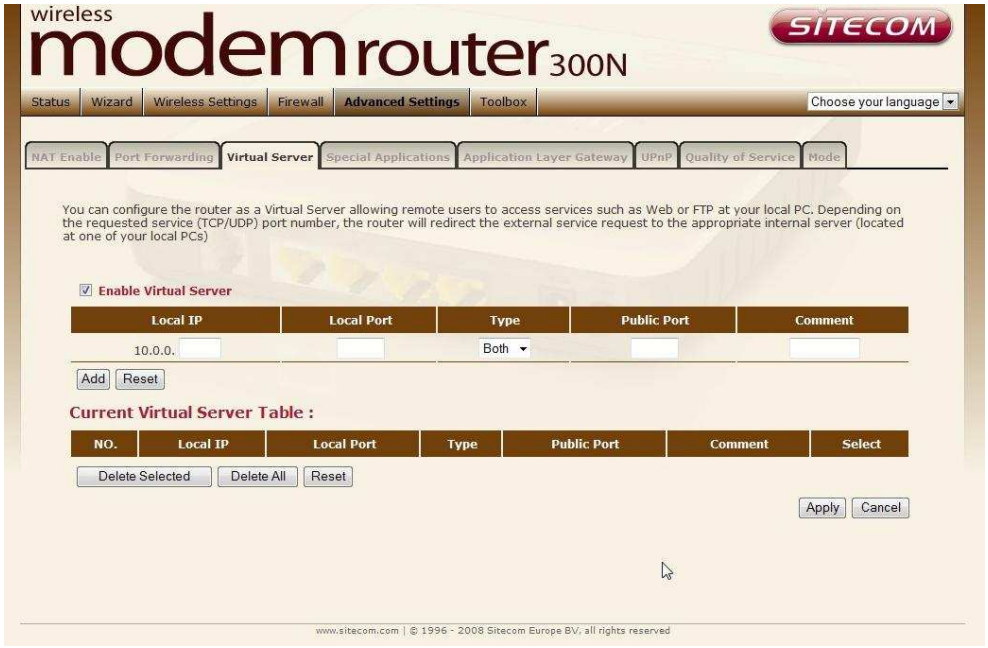
Add Virtual Server Fill in the "Private IP", "Private Port", "Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below.

Remove Virtual Server If you want to remove Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want to remove all Virtual Server settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Virtual server

Use the Virtual Server function when you want different servers/clients in your LAN to handle different service/Internet application type (e.g. Email, FTP, Web server etc.) from the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the Internet/WAN Port) to a particular LAN private IP address and its service port number.



Enable Virtual Server Enable Virtual Server.

Local IP This is the LAN client/host IP address that the Public Port number packet will be sent to.

Local Port This is the port number (of the above Local IP host) that the below **Public Port** number will be changed to when the packet enters your **LAN** (to the LAN Server/Client IP)

Type Select the port number protocol type (TCP, UDP or both). If you are unsure, then leave it to the default "both" setting. Public Port Enter the

service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN

Comment The description of this setting.

Add Virtual Server Fill in the "Private IP", "Private Port", "Type", "Public Port" and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below.

Remove Virtual Server If you want to remove Virtual Server settings from the "Current Virtual Server Table", select the Virtual Server settings you want to remove in the table and then click "Delete Selected". If you want to remove all Virtual Server settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Special application

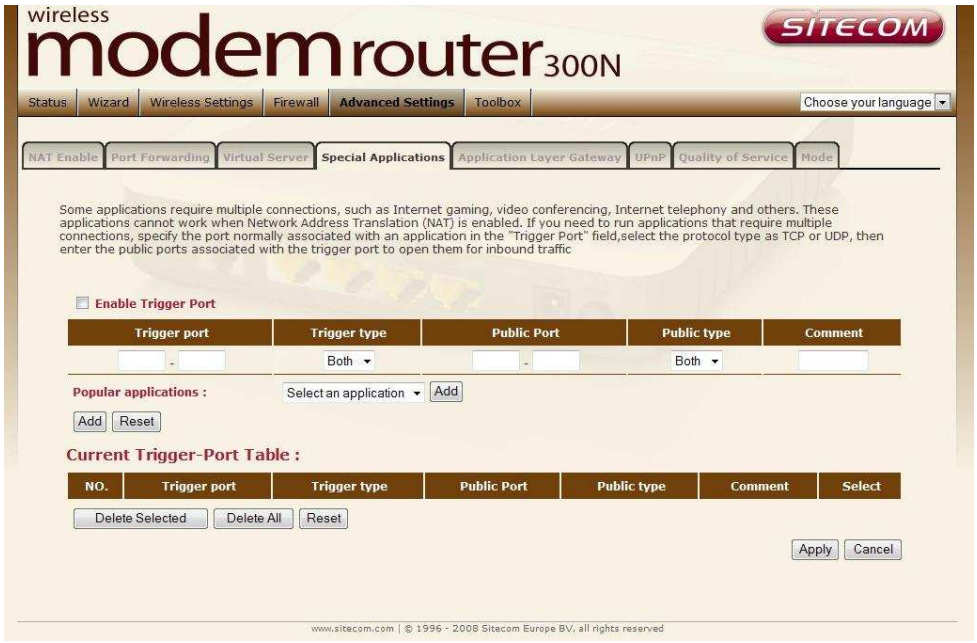
Some applications require multiple connections, such as Internet games, video Conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.

Enable Trigger Port Enable the Special Application function.

Trigger Port This is the out going (Outbound) range of port numbers for this particular application.

Trigger Type Select whether the outbound port protocol is "TCP", "UDP" or both.

Public Port Enter the In-coming (Inbound) port or port range for this type of application (e.g. 2300-2400, 47624)



Public Type Select the Inbound port protocol type: "TCP", "UDP" or both

Comment The description of this setting.

Popular applications This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, select a location (1-10) in the Copy to selection box and then click the Copy to button. This will automatically list the Public Ports required for this popular application in the location (1-10) you specified.

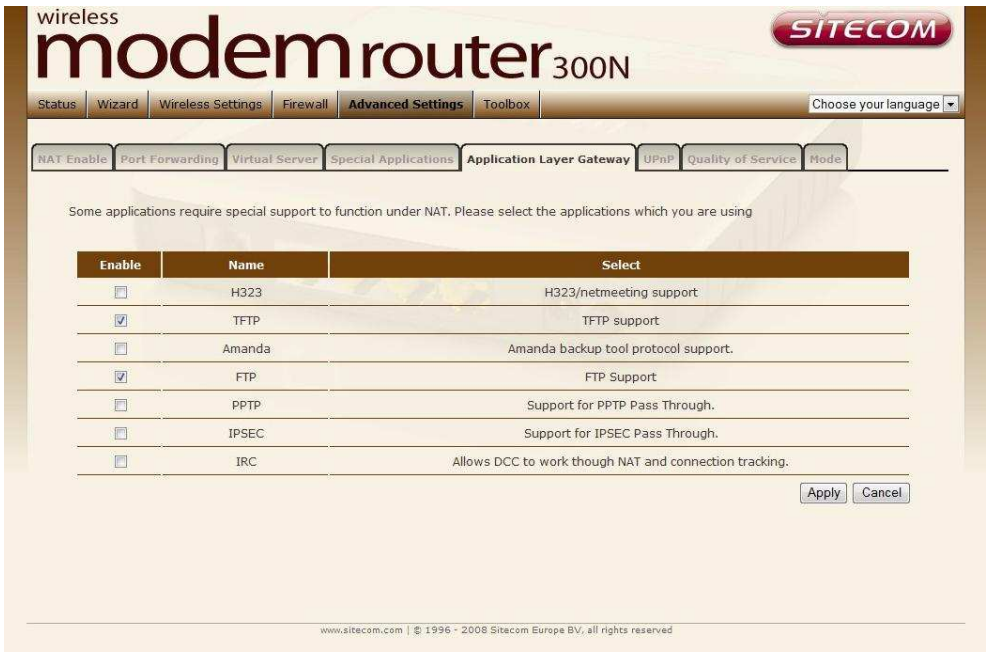
Add Special Application Fill in the "Trigger Port", "Trigger Type", "Public Port", "Public Type", "Public Port" and "Comment" of the setting to be added and then click "Add". The Special Application setting will be added into the "Current Trigger-Port Table" below. If you happen to make a mistake, just click "Clear" and the fields will be cleared.

Remove If you want to remove Special Application settings from the "Current Trigger-Port Table", select the Special Application settings you want to remove in the table and then click "Delete Selected". If you want remove all Special Application settings from the table, just click the "Delete All" button. Click "Reset" will clear your current selections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Application Layer Gateway

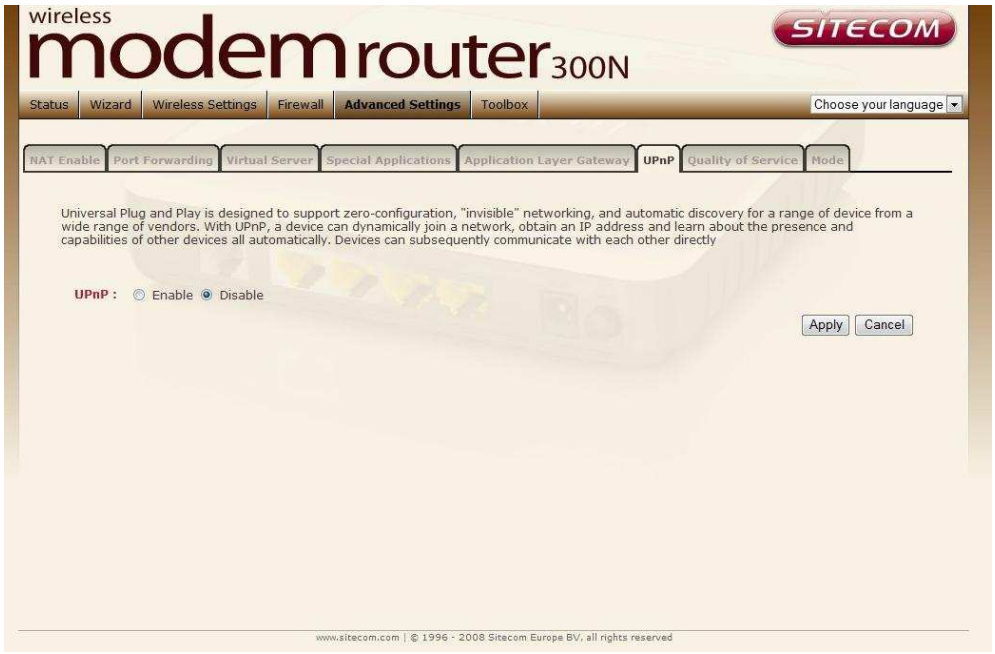
You can select applications that need “Application Layer Gateway” support.



Click <**Apply**> at the bottom of the screen to save the above configurations.

UPNP

With UPnP, all PCs in you Intranet will discover this router automatically. So, you don’t have to configure your PC and it can easily access the Internet through this router.

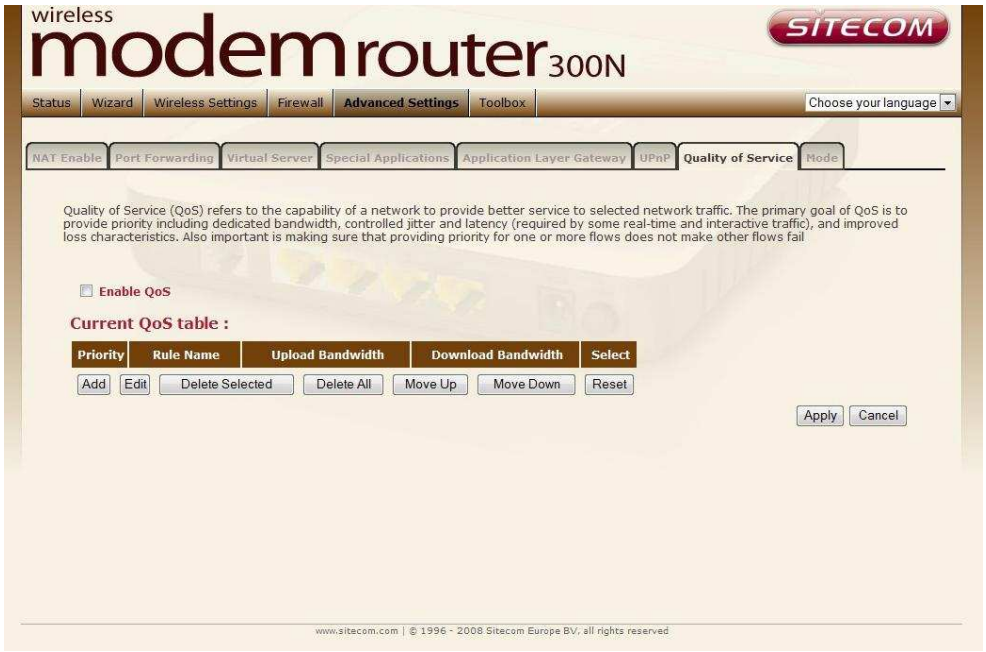

wireless
modem router 300N
SITECOM
Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
NAT Enable
Port Forwarding
Virtual Server
Special Applications
Application Layer Gateway
UPnP
Quality of Service
Mode
Universal Plug and Play is designed to support zero-configuration, "invisible" networking, and automatic discovery for a range of device from a wide range of vendors. With UPnP, a device can dynamically join a network, obtain an IP address and learn about the presence and capabilities of other devices all automatically. Devices can subsequently communicate with each other directly
UPnP :
Enable
Disable
Apply
Cancel
www.sitecom.com | © 1996 - 2008 Sitecom Europe BV, all rights reserved

UPnP Feature You can enable or Disable the UPnP feature here. After you enable the UPnP feature, all client systems that support UPnP, like Windows XP and up, can discover this router automatically and access the Internet through this router without having to configure anything. The NAT Traversal function provided by UPnP can let applications that support UPnP connect to the internet without having to configure the virtual server sections.

Click <**Apply**> at the bottom of the screen to save the above configurations.

QoS

QoS can let you classify Internet application traffic by source/destination IP address and port number. You can assign priority for each type of application and reserve bandwidth for it. The packets of applications with higher priority will always go first. Lower priority applications will get bandwidth after higher priority applications get enough bandwidth. This can let you have a better experience in using critical real time services like Internet phone, video conference …etc. All the applications not specified by you are classified as rule name "Others". The rule with a smaller priority number has a higher priority; the rule with a larger priority number has a lower priority. You can adjust the priority of the rules by moving them up or down.



Enable/Disable QoS You can check "Enable QoS" to enable QoS functionality for the WAN port.

Traffic mapping Click "Add traffic class" then enter a form of the QoS rule. Click "Apply" after filling out the form the rule will be added into the table.

Edit a QoS rule Select the rule you want to edit and click "Edit", then enter the detail form of the QoS rule. Click "**Apply**" after editing the form and the rule will be saved.

Adjust QoS rule priority You can select the rule and click "Move Up" to make its priority higher. You also can select the rule and click "Move Down" to make its priority lower.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Mode

The mode-function allows you to configure the Modem-router as a pure modem, without router functionality.

Note that this feature only works for DHCP and PPPoE internet connections.

Click <**Apply**> at the bottom of the screen to save the above configuration.

14 TOOLBOX Settings

Password change options

You can change the password required to log into the broadband router's system web-based management. Passwords can contain 0 to 12 alphanumeric characters, and are case sensitive.

Current Password Fill in the current password to allow changing to a new password.

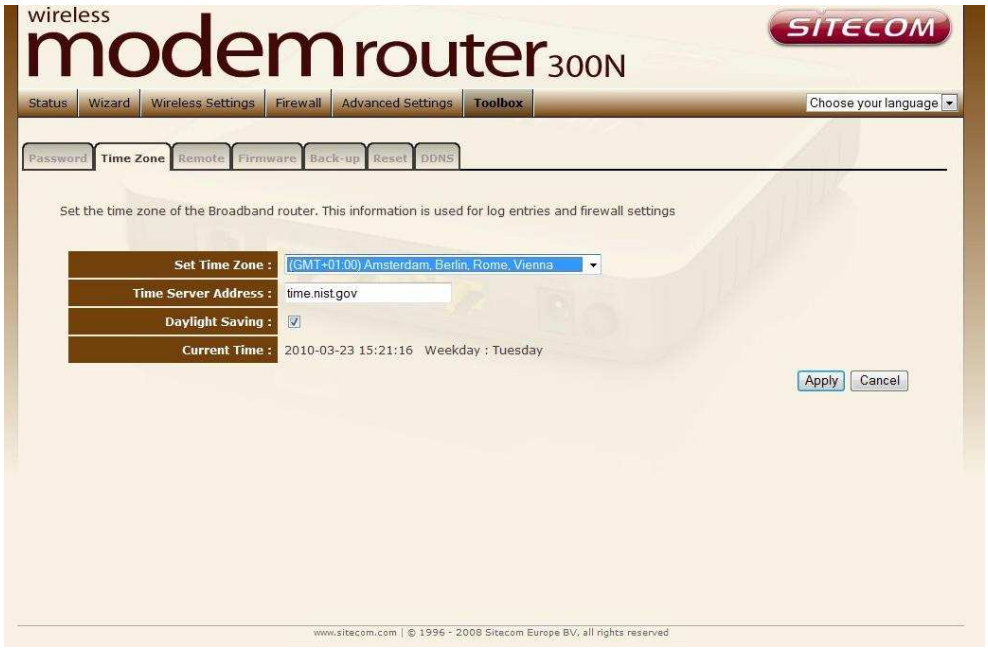
New Password Enter your new password

Confirmed Password Enter your new password again for verification purposes

Click <**Apply**> at the bottom of the screen to save the above configurations

Time Zone

The Time Zone allows your router to base its time on the settings configured here, which will affect functions such as Log entries and Firewall settings.



Set Time Zone Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address You can set an NTP server address.

Enable Daylight Savings The router can also take Daylight savings into account. If you wish to use this function, you must check/tick the enable box to enable your daylight saving configuration (below).

Click <**Apply**> at the bottom of the screen to save the above configurations.

Remote Management

The remote management function allows you to designate a host in the Internet the ability to configure the Broadband router from a remote site. Enter the designated host IP Address in the Host IP Address field.

Host Address This is the IP address of the host in the Internet that will have management/configuration access to the Broadband router from a remote site. If the Host Address is left 0.0.0.0 this means anyone can access the router's web-based configuration from a remote location, providing they know the password.

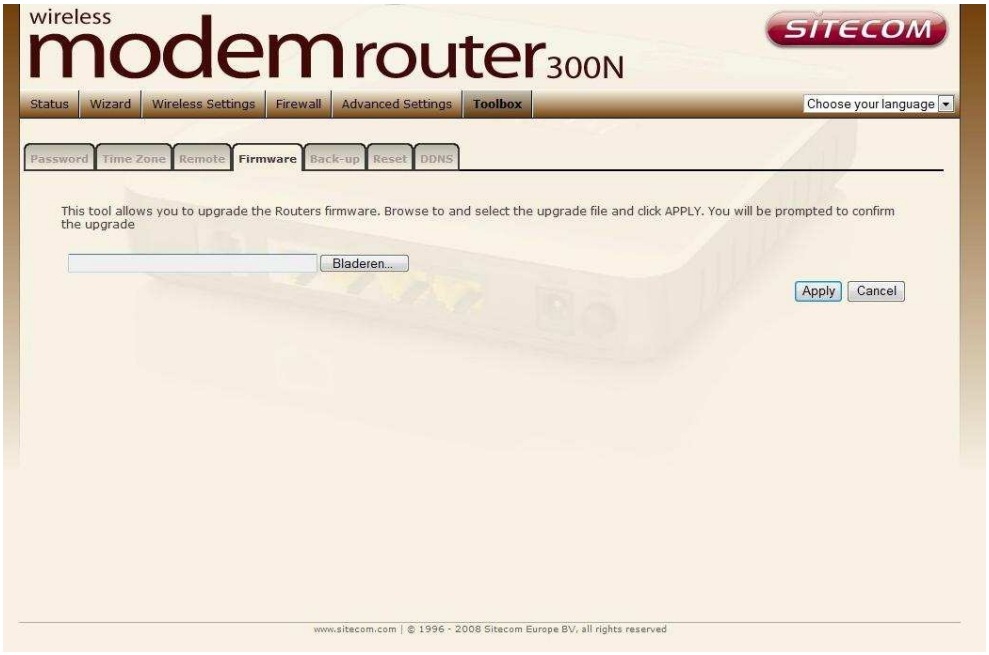
Port The port number of the remote management web interface.

Enabled Select "**Enabled**" to enable the remote management function.

Click <**Apply**> at the bottom of the screen to save the above configurations.

Firmware Upgrade

This page allows you to upgrade the router's firmware.

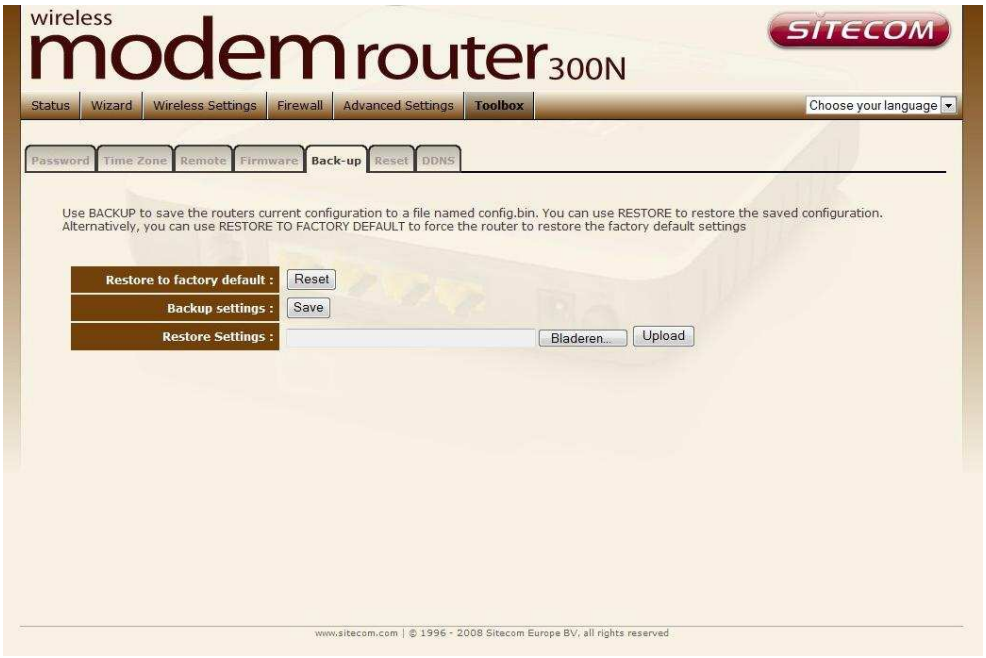


Firmware Upgrade This tool allows you to upgrade the Broadband router's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also use the Browse button to find the firmware file on your PC.

Once you've selected the new firmware file, click <**Apply**> at the bottom of the screen to start the upgrade process

Backup Settings

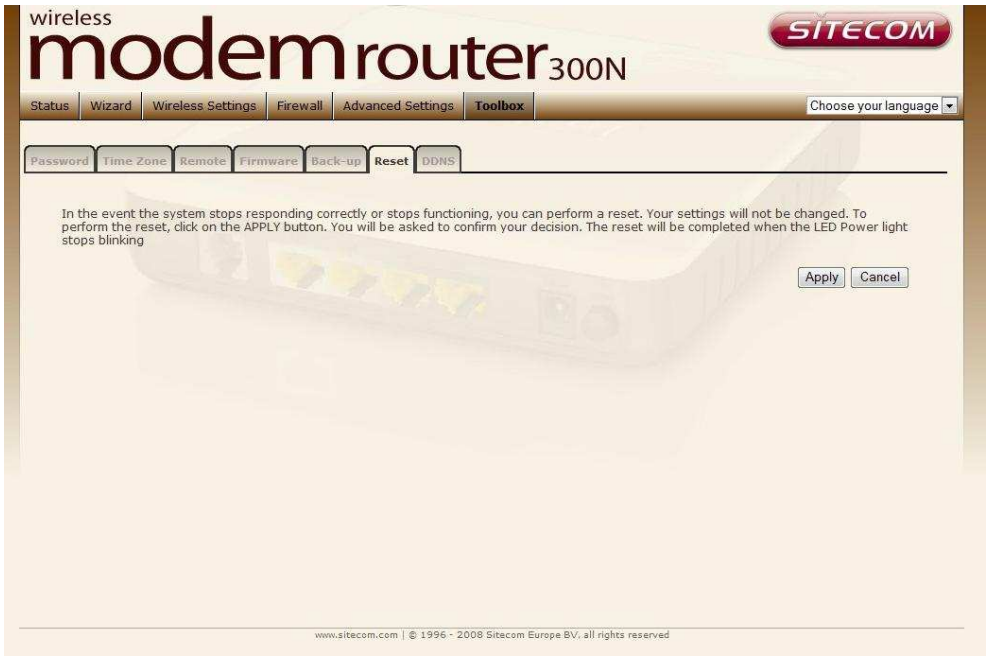
The Backup screen allows you to save (Backup) the router's current configuration settings. When you save the configuration setting (Backup) you can re-load the saved configuration into the router through the Restore selection. If extreme problems occur you can use the Restore to Factory Defaults selection, this will set all configurations to its original default settings (e.g. when you first purchased the router).



Use the "Backup" tool to save the Broadband router current configuration to a file named "**routercfg.cfg**" on your PC. You can then use the "Restore" tool to restore the saved configuration to the Broadband router. Alternatively, you can use the "Restore to Factory Defaults" tool to force the Broadband router to perform a power reset and restore the original factory settings.

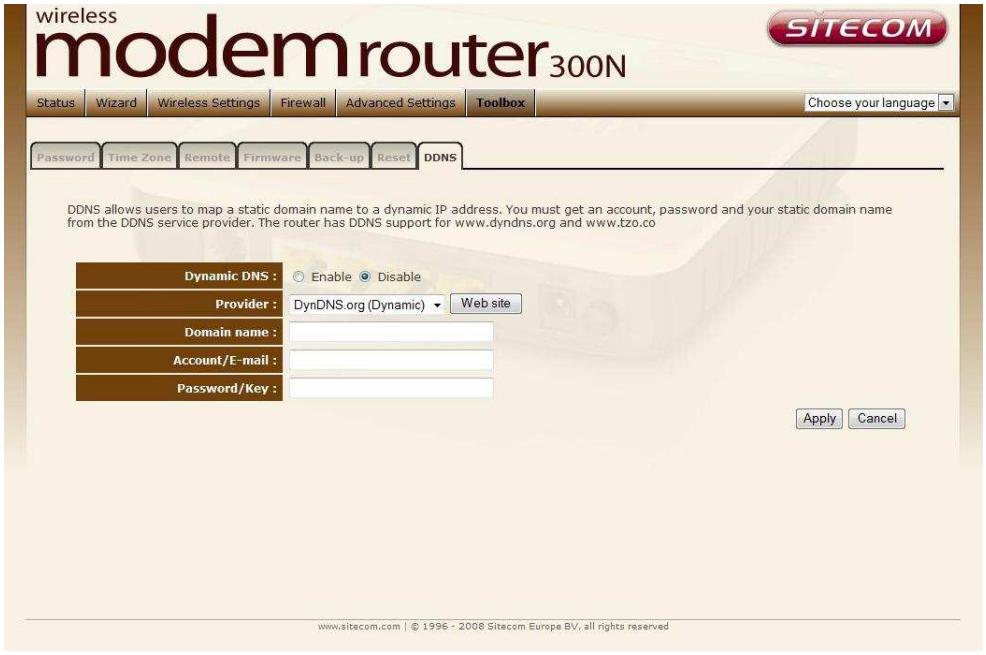
Reset

You can reset the router's system should any problem exist. The reset function essentially re-boots your router's system.


wireless
modem router 300N
SITECOM
Status
Wizard
Wireless Settings
Firewall
Advanced Settings
Toolbox
Choose your language
Password
Time Zone
Remote
Firmware
Back-up
Reset
DDNS
In the event the system stops responding correctly or stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button. You will be asked to confirm your decision. The reset will be completed when the LED Power light stops blinking
Apply
Cancel
www.sitecom.com | © 1996 - 2008 Sitecom Europe BV. all rights reserved

DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS, TZO and other common DDNS service providers.



Enable/Disable Enable or disable the DDNS function of this router

Provider Select a DDNS service provider

Domain name Fill in your static domain name that uses DDNS

Account/E-mail The account that your DDNS service provider assigned to you

Password/Key The password you set for the DDNS service account above

Click <**Apply**> at the bottom of the screen to save the above configurations.